ON THE SUM OF TWO INTEGRAL SQUARES IN QUADRATIC FIELDS $\mathbb{Q}(\sqrt{\pm p})$

DASHENG WEI

Abstract

We propose a method for determining which integers can be written as a sum of two integral squares for quadratic fields $\mathbb{Q}(\sqrt{\pm p})$, where p is a prime.

MSC classification : 11D09; 11E12

Keywords : integral points, ring class field, reciprocity law.

Introduction

Gauss first determined which integers can be written as a sum of two integral squares. And Niven determined which integers can be written as a sum of two integral squares for the imaginary quadratic field $\mathbb{Q}(\sqrt{-1})$ in [11]. Nagell further studied the question for the twenty quadratic fields $\mathbb{Q}(\sqrt{d})$ in [8] and [9], where

$$d = \pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 19, \pm 43, \pm 67, \pm 163.$$

His method essentially depends on the fact that the class number of $\mathbb{Q}(\sqrt{d}, \sqrt{-d})$ is 1 when d is one of the above integers. However, this method can not apply for general quadratic fields. Recently, Harari showed that the Brauer-Manin obstruction is the only obstruction for existence of the integral points of a scheme over a ring of integers of a number field whose generic fiber is a principal homogeneous space of tori in [5]. However, the Brauer-Manin obstruction of tori given in [5] is not constructive and one can not use that result to determine the existence of integral points for the scheme. Fei Xu and the author gave another proof of the result in [17] and [18] which is constructive. In this paper we apply the method in [17] for the question for quadratic fields $\mathbb{Q}(\sqrt{\pm p})$, where p is a prime.

Notation and terminology are standard if not explained. Let F be a number field, $\mathfrak{o}_F$ the ring of integers of F, Ω_F the set of all primes in F and ∞ the set of all infinite primes in F. For simplicity, we write $\mathfrak{p} < \infty$ for $\mathfrak{p} \in \Omega_F \setminus \infty$. Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$ and $\mathfrak{o}_{F_\mathfrak{p}}$ be the local completion of $\mathfrak{o}_F$ at $\mathfrak{p}$ for each $\mathfrak{p} \in \Omega_F$. Write $\mathfrak{o}_{F_\mathfrak{p}} = F_\mathfrak{p}$ for $\mathfrak{p} \in \infty$. We also denote the adele ring (resp. the idele ring) of F by $\mathbb{A}_F$ (resp. $\mathbb{I}_F$) and

$$F_\infty = \prod_{\mathfrak{p} \in \infty} F_\mathfrak{p}.$$

Let $E = F(\sqrt{-1})$ and let T be the torus $R^1_{E/F}(\mathbb{G}_m) = \mathrm{Ker}[R_{E/F}(\mathbb{G}_{m,E}) \to \mathbb{G}_{m,F}]$, here R denotes the Weil's restriction (see [7]). Denote λ to be the embedding from T to $R_{E/F}(\mathbb{G}_{m,E})$. Obviously λ induces a natural group homomorphism

$$\lambda_E : \quad T(\mathbb{A}_F) \to \mathbb{I}_E.$$

Date: April 20, 2010.

Let $\mathbf{X}_\alpha$ be the affine scheme over $\mathfrak{o}_F$ defined by the equation $x^2+y^2=\alpha$ for a non-zero integer $\alpha \in \mathfrak{o}_F$. The generic fiber of $\mathbf{X}_\alpha$ is a principle homogenous space of the torus T. The equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if $\mathbf{X}_\alpha(\mathfrak{o}_F)\neq\emptyset$.

Definition 0.1. Let K/E be a finite abelian extension. Let $\psi_{K/E}:\mathbb{I}_E\to Gal(K/E)$ be the Artin map. We say that α satisfies the Artin condition of K if there is

$$\prod_{\mathfrak{p}\leq\infty}(x_\mathfrak{p},y_\mathfrak{p})\in\prod_{\mathfrak{p}\leq\infty}\mathbf{X}_\alpha(\mathfrak{o}_{F_\mathfrak{p}}) \text{ such that } \psi_{K/E}(f_E[\prod_{\mathfrak{p}\leq\infty}(x_\mathfrak{p},y_\mathfrak{p})])=1$$

where 1 is the identity element of $Gal(K/E)$ and $f_E:\prod_{\mathfrak{p}\leq\infty}\mathbf{X}_\alpha(\mathfrak{o}_{F_\mathfrak{p}})\to\mathbb{I}_E$ is defined by

$$f_E[(x_\mathfrak{p},y_\mathfrak{p})]=\begin{cases}(x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},x_\mathfrak{p}-y_\mathfrak{p}\sqrt{-1}) & \text{if } \mathfrak{p} \text{ splits in } E/F\\ x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1} & \text{otherwise.}\end{cases}$$

By the class field theory, it is a necessary condition for $\mathbf{X}_\alpha(\mathfrak{o}_F)\neq\emptyset$ that α satisfies the Artin condition of K. In fact there is a finite abelian extension K/E that is independent on α, such that the Artin condition of K is also sufficient for $\mathbf{X}_\alpha(\mathfrak{o}_F)\neq\emptyset$ (see [17]).

Let $\mathbf{T}$ be the group scheme over $\mathfrak{o}_F$ defined by $x^2+y^2=1$, which is an integral model of T. Since $\mathbf{T}$ is separated over $\mathfrak{o}_F$, we can view $\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$ as a subgroup of $T(F_\mathfrak{p})$. Furthermore, the following result is proved in [17].

Proposition 0.2. *Let K/E be a finite abelian extension such that the group homomorphism $\widetilde{\lambda}_E$ induced by λ_E*

$$\widetilde{\lambda}_E:{}^{T(\mathbb{A}_F)}\!/_{T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})}\longrightarrow{}^{\mathbb{I}_E}\!/_{E^*N_{K/E}(\mathbb{I}_K)}$$

is well-defined and injective, where well-defined means

$$\lambda_E(T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}))\subset E^*N_{K/E}(\mathbb{I}_K).$$

Then $\mathbf{X}_\alpha(\mathfrak{o}_F)\neq\emptyset$ if and only if α satisfies the Artin condition of K.

In this paper, we mainly prove the following result.

Theorem 0.3. *Let p be a prime number and F the quadratic field $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{-p})$. Then the diophantine equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L, where H_L is the ring class field corresponding to the order $L=\mathfrak{o}_F+\mathfrak{o}_F\sqrt{-1}$.*

1. The sum of two squares in imaginary quadratic fields

Let d be a square-free positive integer here $d\geq 2$. Let $F=\mathbb{Q}(\sqrt{-d})$, $\mathfrak{o}_F$ be the integral ring of F and $E=F(\sqrt{-1})$. One takes the order $L=\mathfrak{o}_F+\mathfrak{o}_F\sqrt{-1}$ inside E. Let H_L be the ring class field corresponding to the order L.

Proposition 1.1. *Suppose one of the following conditions holds:*

(1) The equation $x^2+y^2=-1$ has an integer solution in $\mathfrak{o}_F$.

(2) The equation $x^2+y^2=-1$ has no local integral solutions at a place of F.

Then the diophantine equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L.

Proof. (1) First we assume $d \neq 3$. Let $\mathfrak{p}$ be a place of F and $L_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of L inside $E_{\mathfrak{p}} = E \otimes_F F_{\mathfrak{p}}$. Recall $T = R^1_{E/F}(\mathbb{G}_{m,F})$ and $\mathbf{T}$ is the scheme defined by the equation $x^2 + y^2 = 1$, we have

$$T(F) = \{\beta \in E^* : \ N_{E/F}(\beta) = 1\}$$

and

$$\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}) = \{\beta \in L_{\mathfrak{p}}^{\times} : \ N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}}(\beta) = 1\}.$$

Since the ring class field H_L of the order L corresponds to the open subgroup $E^*(\prod_{\mathfrak{p}\leq\infty} L_{\mathfrak{p}}^{\times})$ of $\mathbb{I}_E$ by the class field theory, the natural group homomorphism

$$\widetilde{\lambda}_E : \quad {}^{T(\mathbb{A}_F)}\!/_{T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})} \longrightarrow {}^{\mathbb{I}_E}\!/_{E^*\prod_{\mathfrak{p}\leq\infty} L_p^{\times}}$$

is well-defined. By Proposition 0.2, we only need to show $\widetilde{\lambda}_E$ is injective.

Suppose there are

$$\beta \in E^* \quad \text{and} \quad i \in E_{\infty}^* \prod_{\mathfrak{p}<\infty} L_{\mathfrak{p}}^{\times}$$

such that $\beta \cdot i \in T(\mathbb{A}_E)$. Then

$$N_{E/F}(\beta i) = N_{E/F}(\beta) N_{E/F}(i) = 1$$

and

$$N_{E/F}(\beta) \in F^* \cap \prod_{\mathfrak{p}<\infty} \mathfrak{o}_{F_{\mathfrak{p}}}^{\times} = \{\pm 1\}.$$

If $N_{E/F}(\beta) = 1$, one concludes that

$$N_{E/F}(\beta) = N_{E/F}(i) = 1 \quad \Rightarrow \quad \beta \in T(E) \quad \text{and} \quad i \in \prod_{\mathfrak{p}\leq\infty} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}).$$

So $\beta i \in T(E)\prod_{\mathfrak{p}\leq\infty} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$.

If $N_{E/F}(\beta) \neq 1$, then $N_{E/F}(\beta) = N_{E/F}(i) = -1$. That is to say that $x^2 + y^2 = -1$ has local integral solutions at every local place of F. By the assumption, we have $x^2 + y^2 = -1$ has an integral solution (x_0, y_0). Let

$$\zeta = x_0 + y_0\sqrt{-1} \ \text{ and } \ \gamma = \beta\zeta, j = i/\zeta.$$

Then $\beta i = \gamma j$ and

$$N_{E/F}(\gamma) = N_{E/F}(j) = 1 \quad \Rightarrow \quad \gamma \in T(F) \quad \text{and} \quad j \in \prod_{\mathfrak{p}} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}).$$

So $\beta i = \gamma j \in T(F)\prod_{\mathfrak{p}\leq\infty} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$. Therefore $\widetilde{\lambda}_E$ is injective.

(2) If $d = 3$, then $\mathfrak{o}_F^{\times} =< \pm 1, \zeta_3 >$, where ζ_3 is a primitive 3-rd root of unity. Since $\zeta_3 = \zeta_3^4$ is a square, we can give a proof for this case with similar arguments as above. □

In the rest of this section we consider the case that d is a prime. First we need the following result that can be found in [16].

Proposition 1.2. *Let p be a prime. Then*
(1) If $p \equiv 1 \mod 4$, then $x^2 - py^2 = -1$ is solvable over $\mathbb{Z}$.
(2) If $p \equiv -1 \mod 8$, then $x^2 - py^2 = 2$ is solvable over $\mathbb{Z}$.
(2) If $p \equiv 3 \mod 8$, then $x^2 - py^2 = -2$ is solvable over $\mathbb{Z}$.

Now we can prove the following lemma.

Lemma 1.3. *Let p be a prime and $F = \mathbb{Q}(\sqrt{-p})$. Then*
(1) If $p \equiv -1 \mod 8$, then $x^2 + y^2 = -1$ is not solvable over $\mathfrak{o}_{F_\mathfrak{p}}$, where $\mathfrak{p} \mid 2$.
(2) If $p \not\equiv -1 \mod 8$, then $x^2 + y^2 = -1$ is solvable over $\mathfrak{o}_F$.

Proof. (1) If $p \equiv -1 \mod 8$, then 2 splits into $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in the field $F/\mathbb{Q}$. So the Hilbert symbol

$$(-1,-1)_{\mathfrak{p}_1} = (-1,-1)_{\mathfrak{p}_2} = -1.$$

Therefore the equation $x^2 + y^2 = -1$ is not solvable over $\mathfrak{o}_{F_{\mathfrak{p}_1}}$ and $\mathfrak{o}_{F_{\mathfrak{p}_2}}$.

If $p \equiv 1 \mod 4$ or $p = 2$, then $x^2 - py^2 = -1$ has an integral solution in $\mathbb{Z}$ by Proposition 1.2. Choose one solution (x_0, y_0), we have $x_0^2 + (y_0\sqrt{-p})^2 = -1$.

If $p \equiv 3 \mod 8$, then $x^2 - py^2 = -2$ has an integral solution in $\mathbb{Z}$ by Proposition 1.2. We can choose one solution (x_0, y_0) and it's easy to see $x_0, y_0 \equiv 1 \mod 2$. So

$$\frac{x_0 \pm y_0\sqrt{-p}}{2} \in \mathfrak{o}_F \text{ and } (\frac{x_0 + y_0\sqrt{-p}}{2})^2 + (\frac{x_0 - y_0\sqrt{-p}}{2})^2 = -1.$$

□

By Proposition 1.1 and Lemma 1.3, we can now prove the following result.

Theorem 1.4. *Let p be a prime number and $F = \mathbb{Q}(\sqrt{-p})$. Let H_L be the ring class field corresponding to the order $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$. Then the diophantine equation $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L.*

Remark 1.5. It is possible that the family of equations $x^2+y^2 = \alpha, \alpha \in \mathfrak{o}_F$ and $\alpha \neq 0$ satisfies Hasse principle even if the ring class field H_L is not trivial. For example, the equation $x^2 + y^2 = \alpha$ satisfies Hasse principle and H_L is not trivial for $F = \mathbb{Q}(\sqrt{-p})$ with $p = 23, 31, 47, 59, 71$. The reason is $H_L = EH$ for the above p, where $E = F(\sqrt{-1})$ and H is the Hilbert class field of F. If $x^2 + y^2 = \alpha$ has local solutions for every place, then α automatically satisfies the Artin condition of H_L by the class field theory.

Now we use Theorem 1.4 to give an explicit example. Let $F = \mathbb{Q}(\sqrt{-79})$. We write $N_{F/\mathbb{Q}}(\alpha) = 2^{s_1}79^{s_2}p_1^{e_1}\cdots p_g^{e_g}$ for any $\alpha \in \mathfrak{o}_F$. Let $D(n) = \{p_1, \cdots, p_g\}$ and $h(x) = x^3 - 307x + 1772$. Denote

$$D_1 = \{p \in D(n) : (\frac{79}{p}) = (\frac{-1}{p}) = 1 \text{ and } h(x) \equiv 0 \mod p \text{ is not solvable}\}$$

$$D_2 = \{p \in D(n) : (\frac{79}{p}) = -(\frac{-1}{p}) = 1 \text{ and } h(x) \equiv 0 \mod p \text{ is not solvable}\}.$$

It's easy to see that e_i is even when $p_i \in D_2$.

Example 1.6. *Let $F = \mathbb{Q}(\sqrt{-79})$ and let α be an integer in F with the above notation. Then $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if*
(1) The equation $x^2 + y^2 = \alpha$ has integral solutions at every place of F.
(2) The sum

$$\sum_{p_i \in D_1} e_i + \sum_{p_i \in D_2} e_i/2 \neq 1.$$

2. The sum of two squares in real quadratic fields

Let d be a square-free positive integer and $F = \mathbb{Q}(\sqrt{d})$. Let $\mathfrak{o}_F$ be the ring of integers of F, ε the fundamental unit of $\mathfrak{o}_F$ and $\varepsilon = a + b\sqrt{d}$ with $a, b > 0$. Let $E = F(\sqrt{-1})$. One takes the order $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$ inside E. Let H_L be the ring class field corresponding to the order L.

Proposition 2.1. *Suppose one of the following conditions holds:*

(1) The equation $x^2+y^2=\varepsilon$ has an integer solution in $\mathfrak{o}_F$.

(2) The equation $x^2+y^2=\varepsilon$ has no local integral solutions at a place of F.

Then the diophantine equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L.

Proof. Let $\mathfrak{p}$ be a place of F and $L_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of L inside $E_\mathfrak{p} = E\otimes_F F_\mathfrak{p}$. Since the ring class field K_L of the order L corresponds to the open subgroup $E^*(\prod_{\mathfrak{p}\leq\infty} L_\mathfrak{p}^\times)$ of $\mathbb{I}_E$ by the class field theory, the natural group homomorphism

$$\widetilde{\lambda}_E: \quad {}^{T(\mathbb{A}_F)}\!/_{T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})} \longrightarrow {}^{\mathbb{I}_E}\!/_{E^*\prod_{\mathfrak{p}\leq\infty} L_p^\times}$$

is well-defined. By Proposition 0.2, we only need to show $\widetilde{\lambda}_E$ is injective.

Suppose there are

$$\beta\in E^* \quad \text{and} \quad i\in E_\infty^*\prod_{\mathfrak{p}<\infty} L_\mathfrak{p}^\times$$

such that $\beta\cdot i\in T(\mathbb{A}_E)$. Then

$$N_{E/F}(\beta i)=N_{E/F}(\beta)N_{E/F}(i)=1$$

and

$$N_{E/F}(\beta)\in F^*\cap\prod_{\mathfrak{p}<\infty}\mathfrak{o}_{F_\mathfrak{p}}^\times=\{\pm\varepsilon^n\}.$$

Since $N_{E/F}(\beta)$ is totally positive, we have $N_{E/F}(\beta)=\varepsilon^n$.

When n is even, let $\gamma=\beta\varepsilon^{n/2}, j=i\varepsilon^{-n/2}$. Then $\beta i=\gamma j$ and

$$N_{E/F}(\gamma)=N_{E/F}(j)=1 \quad\Rightarrow\quad \gamma\in T(F) \quad\text{and}\quad j\in\prod_{\mathfrak{p}}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}).$$

So $\beta i=\gamma j\in T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$.

When n is odd, we have $N_{E/F}(i)=\varepsilon^{-n}$. That is to say that $x^2+y^2=\varepsilon^{-n}$ has integral solutions at every local place of F. Since n is odd and $\varepsilon\in\mathfrak{o}_F^\times$, we have $x^2+y^2=\varepsilon$ has integral solutions at every place of F. By the assumption, we have $x^2+y^2=\varepsilon$ has an integer solution (x_0,y_0). Let $\zeta=x_0+y_0\sqrt{-1}$ and $\gamma=\beta\varepsilon^{(n-1)/2}\zeta, j=i\varepsilon^{(1-n)/2}\zeta^{-1}$. Then $\beta i=\gamma j$. And

$$N_{E/F}(\gamma)=N_{E/F}(j)=1 \quad\Rightarrow\quad \gamma\in T(F) \quad\text{and}\quad j\in\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}).$$

So $\beta i=\gamma j\in T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$. Therefore $\widetilde{\lambda}_E$ is injective. □

In the following, we consider the case that d is a prime number.

Lemma 2.2. *Let p be a prime and $F=\mathbb{Q}(\sqrt{p})$. Let ε be the fundamental unit of $\mathfrak{o}_F$ and $\varepsilon=a+b\sqrt{p}$ with $a,b>0$. Then there is a place $\mathfrak{p}$ of F, such that the equation $x^2+y^2=\varepsilon$ is not solvable over $\mathfrak{o}_{F_\mathfrak{p}}$.*

Proof. If $p\equiv 1 \mod 4$ or $p=2$, then $x^2-py^2=-1$ has integral solutions by Proposition 1.2. Therefore $N_{F/\mathbb{Q}}(\varepsilon)=-1$. There exists a real place $\mathfrak{p}$ of F such that $|\varepsilon|_\mathfrak{p}<0$. So the equation $x^2+y^2=\varepsilon$ is not solvable at the real place $\mathfrak{p}$.

If $p\equiv 3 \mod 4$, then $x^2-py^2=-1$ is not solvable over $\mathbb{Z}$ by Proposition 1.2. Therefore $N_{F/Q}(\varepsilon)=1$ and ε is totally positive. And we know one of the equations $x^2-py^2=\pm 2$ has an integral solution in $\mathbb{Z}$ by Proposition 1.2. We can choose one solution (x_0,y_0) and it is easy to see that x_0 and y_0 are odd. Let

$$A=(x_0^2+py_0^2)/2 \text{ and } B=x_0y_0.$$

Since x_0, y_0 are odd, we can see A, B are integers and B is odd. And

$$A^2 - pB^2 = (x_0^2 - py_0^2)^2/4 = 1.$$

Let $\varepsilon_1 = A + B\sqrt{p}$. Obviously ε_1 is totally positive and $\varepsilon_1 = \varepsilon^m, m \in \mathbb{Z}$.

Let $\mathfrak{p}$ be the unique place of F over 2. We assume the equation $x^2 + y^2 = \varepsilon$ is solvable over $\mathfrak{o}_{F_\mathfrak{p}}$. Since $\varepsilon_1 = \varepsilon^m$, the equation $x^2 + y^2 = \varepsilon_1$ is also solvable over $\mathfrak{o}_{F_\mathfrak{p}}$. For any solution $(x_1, y_1) = (a_1 + b_1\sqrt{p}, a_2 + b_2\sqrt{p})$, we have

$$(a_1 + b_1\sqrt{p})^2 + (a_2 + b_2\sqrt{p})^2 = A + B\sqrt{p}.$$

Then

$$2a_1b_1 + 2a_2b_2 = B.$$

However, we know B is odd, a contradiction is derived. □

By Proposition 2.1 and Lemma 2.2, we can now prove the following result.

Theorem 2.3. *Let p be a prime number and $F = \mathbb{Q}(\sqrt{p})$. Let H_L be the ring class field corresponding to the order $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$. Then the diophantine equation $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L.*

Now we use Theorem 2.3 to give an explicit example. Let $F = \mathbb{Q}(\sqrt{17})$. We write $N_{F/\mathbb{Q}}(\alpha) = 2^{s_1}17^{s_2}p_1^{e_1}\cdots p_g^{e_g}$ for any $\alpha \in \mathfrak{o}_F$. Let $D(n) = \{p_1, \cdots, p_g\}$ and $h(x) = x^4 - 2x^2 + 17$. Denote

$$D_1 = \{p \in D(n) : (\frac{-17}{p}) = -(\frac{-1}{p}) = 1\}$$

$$D_2 = \{p \in D(n) : (\frac{-17}{p}) = (\frac{-1}{p}) = 1 \text{ and } h(x) \equiv 0 \mod p \text{ is not solvable}\}.$$

We can see e_i is even if $p_i \in D_1$.

Example 2.4. *Let $F = \mathbb{Q}(\sqrt{17})$ and let α be an integer in F with the above notation. Then $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if*

(1) The equation $x^2 + y^2 = \alpha$ has integral solutions at every place of F.

(2) The sum

$$s_1 + \sum_{p_i \in D_1} e_i/2 + \sum_{p_i \in D_2} e_i \equiv 0 \mod 2.$$

Acknowledgment *The author would like to thank Fei Xu and Chungang Ji for some helpful discussions. The work is supported by the Morningside Center of Mathematics and NSFC, grant # 10901150 and # 10671104.*

References

[1] D.A.Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, Inc., 1989.

[2] J-L.Colliot-Thélène and F. Xu, *Brauer-Manin obstruction for integral points of homogeneous spaces and representations by integral quadratic forms*, Compositio Math. **145** (2009), 309–363.

[3] G.L.Dirichlet, *Einige neue sätze über unbestimmte gleichungen*, "Werke" **I** (1920), 221–236.

[4] P.Epstein, *Zur auflösbarkeit der gleichung $x^2 - Dy^2 = -1$*, J. reine und angew. Math. **171** (1934), 243 –252.

[5] D. Harari, *Le défaut d'approximation forte pour les groups algébriques commutatifs*, Algebra and Number Theory **2** (2008), no. 5, 595–611.

[6] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press, 1986.

[7] ———, *Algebraic geometry*, World Scientific Publishing Co., 1998.

[8] T. Nagell, *On the representations of integers as the sum of two integral squares in algebraic, mainly quadratic fields*, Nova Acta Soc. Sci. Upsal. (4) **15** (1953), no. 11, 77pp.

[9] ———, *On the sum of two integral squares in certain quadratic fields*, Ark. Mat. **4** (1961), 267–286.
[10] J.Neukirch, A.Schmidt, and K.Wingberg, *Cohomology of number fields*, Grundlehren, vol. 323, Springer, 2000.
[11] I. Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. **48** (1940), no. 3, 405–417.
[12] O.T.O'Meara, *Introduction to quadratic forms*, Springer -Verlag, 1973.
[13] V. P. Platonov and A. S. Rapinchuk, *Algebraic groups and number theory*, Academic Press, 1994.
[14] L.Rédei, *Über die Pellsche gleichung* $t^2 - du^2 = -1$, J. reine und angew. Math. **173** (1935), 193 –221.
[15] A. N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, 2001.
[16] H. Yokoi, *Solvability of Diophantine equation* $x^2 - Dy^2 = \pm 2$ *and new invariants for real quadratic fields*, Nagoya Math. J. **134** (1994), 137 –149.
[17] D. Wei and F. Xu, *Integral points for multi-norm tori*, arXiv:1004.2608.
[18] ———, *Integral points for groups of multiplicative Type*, arXiv:1004.2613.

Academy of Mathematics and System Science, CAS, Beijing 100190, P.R.China
E-mail address: dshwei@amss.ac.cn